



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/585,665	06/01/2000	Thomas Anthony Parker	190-1457	4497

7590 11/28/2003

Lee Mann Smith McWilliams Sweeney and Ohlson
P O Box 2786
Chicago, IL 60690-2786

EXAMINER

TRAN, TONGOC

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 11/28/2003

5

Please find below and/or attached an Office communication concerning this application or proceeding.

5

Office Action Summary

Application No.

09/585,665

Applicant(s)

PARKER, THOMAS ANTHONY

Examiner

Tongoc Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 01 June 2000.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 and 6-10 is/are rejected.
- 7) ☐ Claim(s) 5 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 3,4.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's application serial no. 09/585,665 filed on 6/1/2000.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 6/1/2000 and 6/12/2003 has been considered by the examiner.

Priority

3. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Claim Objections

4. Claim 5 is objected to because of the following informalities:
Page 17, line 2, missing ",", between "message key" and "a special key".
Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 4, the phrase "a said message" is unclear whether applicant is intended to refer to "a message" or "said message".

In claim 5, the phrases " a said node" is unclear whether applicant is intended to refer to "the first node" or "the second node".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

7. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

8. Claims 1-4, 6 and 9 are rejected under 35 U.S.C. 102(e) as being anticipated by Caronni et al. (U.S. Patent No. 5,822,434 hereinafter Caronni).

9. In respect to claim 1, Caronni discloses a computer system comprising a first node, a second node and a communications link connecting the first node and the second node, and wherein initially the system is capable of working in a plurality of modes, including a first mode corresponding to in clear working over the link (see col. 1,

Art Unit: 2134

lines 14-21 and col. 3, lines 55-57), a second mode corresponding to encrypted working over the link (see col. 3, lines 48-54 and col. 4, lines 49-51), and a third mode employed for migration from in-clear to encrypted working over the link, and wherein the third mode provides in-clear working until means required for encrypted working are provided at both the first and the second nodes, when encrypted working is commenced and from which point in time only encrypted working is possible over the link (see col. 2, lines 57, col. 4, lines 57-61 and col. 7, lines 28-39).

10. In respect to claim 2, Caronni discloses a computer system comprising a first node, a second node and a communications link connecting the first node and the second node, wherein the system is initially capable of operating in a plurality of modes, including a first mode corresponding to in-clear working over the link (see col. 1, lines 14-21 and col. 3, lines 55-57), a second mode corresponding to encrypted working over the link (see col. 3, lines 48-54 and col. 4, lines 47-51), and a third mode, employed for migration from in-clear working over the link to encrypted working over the link, in which one said node is set to "initiate encryption" and the other said node is set to "accept encryption", and wherein the third mode provides in-clear working until means required for encrypted working are installed at both the first and the second nodes, when encrypted working is provided over the link and from which point in time only encrypted working is possible over the link (see col. 2, lines 57-67, col. 4, lines 57-61 and col. 7, lines 28-39).

11. In respect to claim 3, Caronni discloses a computer system as claimed in claim 2, wherein the means required for encrypted working comprise a long term key, which long

Art Unit: 2134

term key is used to establish a message encryption key to be employed by the first and the second nodes for encryption and decryption of messages transmitted over the link (see col. 5, lines 3-19).

12. In respect to claim 4, Caronni discloses computer system as claimed in claim 3, wherein the first and second nodes each include a respective cache, in both of which caches a said message encryption key is stored upon its establishment (see col. 5, lines 11-12).

13. In respect to claim 6, discloses a computer system as claimed in claim 2 and wherein each said node includes policy files for controlling setting to one of the three modes of operation (see col. 2, lines 57-67, col. 3, line 65-col. 4, line 5).

14. In respect to claim 9, Caronni discloses a method for use in migrating operation of a computer system from in-clear working to encrypted working, the computer system comprising a first node, a second node and a communications link connecting the first and second nodes, the computer system initially being capable of operating in a plurality of modes including "in-clear" mode (see col. 1, lines 14-21 and col. 3, lines 55-57), migration mode having settings of "initiate encryption" or "accept encryption" (see col. 2, lines 57-67), and "encrypt" mode (see col. 4, lines 49-51), means enabling encrypted working being required to be installed at the first and second nodes before encrypted working can commence, the method including the steps of installing said means at the first node, setting the first node to "initiate encryption", setting the second node to "accept encryption", as a result of which messages transmitted between said nodes are transmitted in-clear, subsequently installing said means at the second node, as a result

Art Unit: 2134

of which messages between the nodes are transmitted encrypted, and setting the first and second nodes to "encrypt" mode whereby only encrypted working is subsequently possible over the link (see col. 2, lines 57-67, col. 4, lines 57-61, col. 7, lines 28-39).

Claim Rejections - 35 USC § 103

15. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

16. Claims 7-8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caronni et al. (U.S. Patent No. 5,822,434) in view of Arrow et al. (U.S. Patent No. 6,226,751).

17. In respect to claim 7, Caronni discloses a computer system including at least one central server and at least one remote client connectable by a shared network, wherein the or each server and the or each client include respective security policy files with settings of "in-clear", "initiate encryption" or "accept encryption", and "encrypt" for information to be transmitted there between (see col. 2, lines 57-67, col. 3, line 65-col. 4, line 5), "in-clear" corresponding to a mode of operation, comprising working in-clear (see col. 1, lines 14-21, col. 3, lines 55-57), "encrypt" corresponding to a mode of operation comprising encrypted working over the network (see col. 3, lines 48-54 and col. 4, lines 49-51), and "initiate encryption" or "accept encryption", being employed for a mode of operation when migration from in-clear to encrypted working is required,

which migration mode provides in-clear working until authentication keys required for encrypted working are installed at both ends of a particular server/client link across the network, when encrypted working is provided for said link and from which point in time only encrypted working is possible over said link (see col. 2, lines 57-67, col. 4, lines 57-61 and col. 7, lines 28-39, col. 5, lines 3-19). Caronni does not disclose said computer system capable of operation as a virtual private network (VPN). However, Arrow discloses a method and system for establishing a virtual private network that operates over a public data network (see Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Caronni's teaching of allowing two computers on a network to upgrade from a non-secured to a secured session with Arrow's teaching of establishing a virtual private network that operates over a public data network in order to facilitating secure communications across a public network that is able to selectively encrypt and decrypt communications based upon the identities of entities that are sending and receiving (see col. 3, lines 1-5).

18. In respect to claim 8, Caronni and Arrow disclose a computer system as claimed in claim 7. Caronni further discloses including means serving to reset the security policy files at both ends of the link to "encrypt" from "initiate encryption" or "accept encryption", in response to receipt of a message indicating installation of the authentication keys at both ends of said link (see col. 2, line 51-col. 3, line 3).

19. In respect to claim 10, Caronni discloses method for use in migrating operation of a computer system, comprising at least one central server and at least one remote

client connectable by a shared network, including the step of providing the or each server and the or each client with respective security policy files having settings for "in-clear", "initiate encryption" or "accept encryption", and "encrypt" for information to be transmitted there between (see col. 2, lines 57-67, col. 3, line 65-col. 4, line 5), "in-clear" corresponding to a mode of operation comprising working in-clear (see col. 1, lines 14-21, col. 3, lines 55-57), "encrypt" corresponding to a mode of operation comprising encrypted working over the network (see col. 3, lines 48-54 and col. 4, lines 49-51), and "initiate encryption" or "accept encryption" corresponding to a mode of operation which is employed when migration from in-clear to encrypted working is required and which provides in-clear working until authentication keys required for encrypted working are installed, and including the steps of setting the policy file on the server of a particular link to "initiate encryption" and setting the policy file on the client of said particular link to "accept encryption" when migration is required (see col. 2, lines 57-67, col. 4, lines 57-61 and col. 7, lines 28-39), installing the authentication key at the server of said particular link, messages between the server and the client of the particular link thereby being transmitted in clear, subsequently installing the authentication keys at the client of said particular link whereby encrypted working commences instead of in-clear working, and resetting the security policy files of the server and client of said particular link to "encrypt" whereby only encrypted working is subsequently possible over said link (see col. 2, line 57-col. 3, line 3 and col. 5, lines 3-19).

Caronni does not disclose connecting shared network from in-clear working to virtual private network (VPN) work. However, Arrow discloses a method and system for

Art Unit: 2134

establishing a virtual private network that operates over a public data network (see Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Caronni's teaching of allowing two computers on a network to upgrade from a non-secured to a secured session with Arrow's teaching of establishing a virtual private network (VPN) that operates over a public data network (in-clear working) in order to facilitating secure communications across a public network that is able to selectively encrypt and decrypt communications based upon the identities of entities that are sending and receiving (see col. 3, lines 1-5).

Allowable Subject Matter

Claim 5 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

A computer system as claimed in claim 4, wherein when there is a failure to establish a said message encryption key a special key value is cache in the cache of a node set to "initiate encryption:", the presence of which special key value serve to suspend attempts to establish a said message encryption key.

Conclusion

Art Unit: 2134

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Arrow et al. disclose a method and apparatus for swapping a computer operating system.

-Bots et al. disclose an architecture for virtual private networks.

-Howard et al. disclose a method and system for secure network policy implementation.

-Gilbrech discloses an apparatus for implementing virtual private networks.

-Branscome discloses synchronous digital data scrambling system.

-Peyravian et al. disclose decentralized systems methods and computer program products for sending secure messages among a group of nodes.

-Lund et al. disclose a method and arrangement for establishing an encrypted modile connection.

-Chen et al. disclose a multi-access virtual private network.

-Muniyappa et al. disclose method and apparatus for providing a virtual private network.

-Brown et al. disclose secure communication system having long-term keying variable.

-Smith Sr. et al. disclose a method and apparatus for validating entry of cryptographic keys.

-Campbell, Jr. discloses a key variable generator for an encryption/decryption device.

Art Unit: 2134

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-9600.

Examiner Tongoc Tran
Art Unit: 2134

TT
November 5, 2003

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2134